

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,066	04/26/2001	Michael D. Doyle	021117-000200US	9586

7590 09/30/2004
Edward J. Radlo
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306

EXAMINER

GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 09/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/844,066	Applicant(s) DOYLE ET AL.	
	Examiner Tom Gyorfi	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>7/5/02</u> . | 6) <input type="checkbox"/> Other: ____ |

1. Claim 1 has been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guski (U.S. Patent 6,711,679), and further in view of Doyle (PCT Patent WO 99/16209).

Regarding claim 1, Guski teaches a system to perform a serially chained certification process (Guski, column 3 line 57 – column 4, line 4) which comprises the steps of having a second server perform a cross-certification such that the first server must provide independent proof of its public key, in the form of the digital signature which only it could produce with a corresponding private key, at a point in time witnessed by the first server (Guski, Figure 3 and also column 7, lines 15-20); and also continuing the process to cross-chain an unlimited number of additional servers to form a widely witnessed web of digital signatures (Guski, Figure 4 and column 8, lines 9-20). It does not teach the use of time intervals and associated public/private key pairs as part of its certification process. However, Doyle teaches a system for creating irrefutable digital signature timestamps based on the notion of creating public and private key pairs for a number of time intervals. In particular, Doyle teaches the steps of creating a first interval certification at a server (Doyle, page 13, lines 8-12) and deleting

Art Unit: 2135

the private key of the interval once the interval has expired (Doyle, page 6, lines 6-10 and also page 19, lines 26-27). It is also taught that the process can be repeated for additional intervals (Doyle, page 13, lines 15-16), creating a chain of irrefutable timestamps bearing witness to the interval of time thus certified (Doyle, page 19, lines 18-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the concept of temporal intervals as part of the certification process taught by Guski, as well as using the public and private key pairs associated with said intervals as the keys used in the digital signatures contained in the certificates found in the Guski disclosure. Note that the intended purpose of the Guski disclosure was to improve the security of E-commerce transactions, particularly those conducted through the use of intermediaries (Guski, column 3, lines 3-22); by including accurate timestamps as found in Doyle, one can more easily detect a hacker attempting a replay attack against the system – if the timestamp in the certificate does not match that logged by the network hardware on the server, then the contents of the message could then be viewed as suspect.

Further regarding claim 1, note that the only components of the certificates explicitly taught by either Guski or Doyle are the server information (in the form of a server certificate), expiration date/stop time of the interval (Guski, column 7, lines 27-31), the public key of the interval and a digital signature of the submitted data, signed by the interval's private key (Doyle, page 13, lines 8-12 and also lines 18-20). The start time of an interval chain in UTC and the start time of the interval in UTC are not elements of the certificate taught by either reference. However, it would have been

Art Unit: 2135

obvious to one of ordinary skill in the art at the time the invention was made to include those elements as part of the certificate. Possessing this information would make it easier for an authenticator to verify that the timestamp does indeed belong to the interval that signed it.

Further regarding claim 1, note that a digital signature for the interval signed by the previous interval's private key is not explicitly taught, although it should be noted that the public key representing the current interval is signed by the previous interval's private key (Doyle, page 18, lines 13-17). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include information about the current interval in the digital signature of the public key that is already included in the certificate. Since the intervals are well-defined units of time (Doyle, page 11, lines 4-5) and each interval begins when the previous interval ends, any given interval has enough information about the next interval to encode it with the public key signature; further, by including this information, one can be more certain that the public key supplied in the certificate does indeed belong to the new interval immediately succeeding the previous one, and that the key is not in fact a valid public key that was supplied out of sequence.

Conclusion

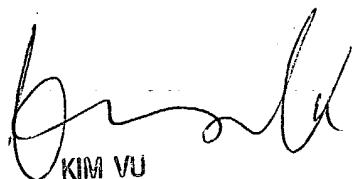
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
09/27/04



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100